

XSS

Cross-site scripting

Kamila Środa

General idea - Cross Site Scripting (XSS)

- a code injection attack allowing the injection of malicious code into a website
- one of the most common website attack with almost every website requiring the user to have Javascript turned on
- it uses the website as a means to attack the users of that website
- when you get your XSS permanently on a website, all those who visit that page will have the javascript executed by their browsers

How web pages work

- web is based on HTML - HyperText Markup Language
- tags in a html document - anything between angle brackets is read as an instruction: `<html> ... </html>`
- escaping - **<** instead of `<`
- later.. interactivity - the invention of JavaScript

```
1  <!DOCTYPE html>
2  <html>
3  <head>
4    <title>Title</title>
5  </head>
6  <body>
7    <h1> My page </h1>
8    <div> Content </div>
9  </body>
10 </html>
```

JavaScript

- programming language, in the middle of web pages
- nothing from the section inside the `<script> ... </script>` will actually appear on the user's screen
- possibilities!
 - declaring variables
 - making calculations
 - operating on DOM - Document Object Model
- language that can affect your document
- powerful = dangerous

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <title>Title</title>
5 </head>
6 <body>
7   <h1> My page </h1>
8   <div> Content </div>
9
10  <script>
11    console.log('do magic!')
12  </script>
13
14 </body>
15 </html>
```




Log in to Citibank® Online

Log in☐ Remember my User IDForgot your [User ID](#) or [Password](#) ?Aren't you our account holder yet? [Register for online banking.](#)



Bezpierczna | <https://www.google.pl>



Szukaj w Google

Szcęśliwy traf



Bezpierczna | https://www.google.pl

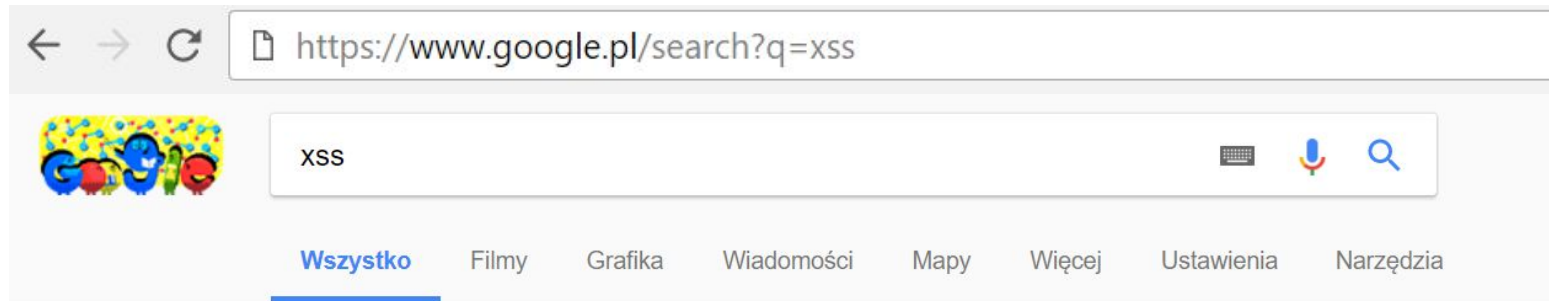


xss



Szukaj w Google

Szcęśliwy traf



Okolo 10 900 000 wyników dla **xss**

Cross-site scripting - Wikipedia

https://en.wikipedia.org/wiki/Cross-site_scripting ▼ Tłumaczenie strony

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. **XSS** enables attackers to inject client-side scripts into ...

Ta strona została przez Ciebie odwiedzona w dniu 14.10.17.

Cross-site Scripting (XSS) - OWASP

[https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)) ▼ Tłumaczenie strony

4 cze 2016 - **Cross-Site Scripting (XSS)** attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites.

Wyszukiwania podobne do: **xss**

xss **example**

cross site scripting przykład

xss **zabezpieczenie**

dom based xss



<i> test



Szukaj w Google

Szczęśliwy traf



<i> test



Wszystko

Grafika

Filmy

Mapy

Zakupy

Więcej

Ustawienia

Narzędzia

Okolo 1 960 000 000 wyników (0,53 s)

iTest: Automated CLI, Call Quality and Performance Testing

www.i-test.net/ ▼ Tłumaczenie strony

Test your VoIP routes with iTest, for Call Quality and performance testing.

[iTest:How it works](#) · [News](#) · [About Us](#)

I test - Tłumaczenie na polski - angielskich przykładów | Reverso Context

context.reverso.net/tlumaczenie/angielski-polski/I+test ▼

Tłumaczenia w kontekście hasła "I test" z angielskiego na polski od Reverso Context: type i test.

IQ Test EU – Testujemy IQ UE

www.iq-test.pl/ ▼

Dlaczego wykonać właśnie ten test IQ? Został on przygotowany przez liderów na polu inteligencji.

Dzięki dużej liczbie przetestowanych osób ocena jest bardziej ...

[Testy aktualnie dostępne](#) · [FAQ](#) · [Statystyki UE - IQ](#) · [Historia](#)

Do I Test

www.doitest.org/ ▼ Tłumaczenie strony

Do I Test. TASC Logo. Enter your PIN number and date of birth to see if you need to test today. PIN:

Date of Birth (mmddyy):. Check it! Get it on Google Play. Back ...

What can we do with XSS?

- it can be used to steal cookies, allowing for someone to use the website pretending to be that user
- we can modify the page to make it look differently or behave differently, for instance change links to malware downloads
- we can send user to another website where his/her login data will be phished

Demo 1

Non-persistent XSS (Reflected)

- most common type of XSS
- the attacker's payload script has to be part of the request to some vulnerable part of the site, and the site renders the javascript on the page
- the attacker needs to deliver the payload to each victim – social networks are often conveniently used for the dissemination of these attacks
- using Phishing emails and other social engineering techniques, the attacker lures the victim to make a request to the server which contains the XSS payload and ends-up executing the script that gets reflected and executed inside the browser

Demo 2

Persistent XSS (Stored)

- the most damaging type of XSS
- it involves an attacker injecting a script that is permanently stored (persisted) on the target application (for instance within a database)
- a classic example is a malicious script inserted by an attacker in a comment field on a blog or in a forum post
- when a victim navigates to the affected web page in a browser, the XSS payload will be served as part of the web page (just like a legitimate comment would). This means that victims will inadvertently end-up executing the malicious script once the page is viewed in a browser



How can we protect against XSS?

XSS Prevention Cheat Sheet

OWASP - Open Web Application Security Project

7 RULES

[https://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

Famous XSS worms

Samy worm

- an XSS worm that was designed to propagate across the MySpace
- within just 20 hours of its October 4, 2005 release, over one million users had run the payload making Samy the fastest spreading virus of all time
- the worm itself was relatively harmless, it carried a payload that would display the string "but most of all, samy is my hero" on a victim's MySpace profile page as well as send Samy a friend request
- when a user viewed that profile page, the payload would then be replicated and planted on their own profile page continuing the distribution of the worm.
- MySpace has since secured its site against the vulnerability

Justin.tv worm

- Justin.tv is a video casting website with an active user base of approximately 20 thousand users
- The cross-site scripting vulnerability that was exploited was that the "Location" profile field was not properly sanitized before its inclusion in a profile page

Hotmail worm

- The vulnerability enabled hackers to display a message that looked like a Facebook notification warning the victim's account had been accessed from a new location
- Embedded in the message was a script that forwarded the victim's e-mail messages to the hackers

Thank you

Sources

- <https://www.acunetix.com/websitesecurity/xss/>
- XSS Tutorials -
https://www.youtube.com/watch?v=M_nllcKTxGk&list=PL1A2CSdiySGIRec2pvDMkYNi3iRO89Zot
- Cracking Websites with Cross Site Scripting - Computerphile -
<https://www.youtube.com/watch?v=L5l9ISnNMxg>
- https://pl.wikipedia.org/wiki/Cross-site_scripting
- [https://en.wikipedia.org/wiki/Samy_\(computer_worm\)](https://en.wikipedia.org/wiki/Samy_(computer_worm))
- [https://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)